홈네트워크 환경에서의 멀티미디어 디지털 컨텐트 권한 관리 모델에 관한 연구

The Study of Models for Multimeia Digital rights Managements in Home Network

정종진, 김윤상, 임태범, 이석필
Jung, Jong-Jin, Kim, Yun-Sang, Lim, Tae-Bum, Lee, Suk-Pil

Abstract - Due to the rapid popularization of mobile multimedia devices and the Internet as well as the realization of high-speed data transmission and large-volume data recording media, high quality content distribution and ubiquitous information services are making progress and a new type of information distribution and network sharing service has gradually emerged into the market. It is capable of utilizing terabyte sized home servers also in private homes.

Under these circumstances, in distribution of content over shared networks, it is crucial to establish DRM (Digital Rights Management) technologies to protect the content from illegal copying and usage. A truly successful DRM system must be built on open worldwide specifications and provide maximum interoperability and user acceptance. An open interoperability of DRM is able to construct highly expandable PKI based DRM, targeting usage between systems, considering the expansion of recent content distribution services and clients This document gives protocol specifications for the exchange of rights information between the DRM module, description of specifications for rights information and encrypted content formats.

Key Words :DRM, 상호연동(Interoperability), TLS, SLM

1. 장 서 론

최근 멀티미디어, 인터넷, 정보통신기술의 발달로 인해 고품질 멀티미디어 컨텐트가 증대되고 있고, 이를 대형 단말기뿐만 아니라 소형 단말기에서 손쉽게 시청 가능해지고 있다. 개인별로 소형단말기 보유가 늘어남에 따라 가정내에서 홈네트웍을 구성하여 개인용 단말기와 홈서버간에 컨텐트와 Data를 서로 주고 받으며 시청 및 컨텐트 이동등을 할 수 있는 멀티미이더 홈네트웍 서비스에 대한 연구 및 개발이 한창 진행중에 있다. 또한 큰비용을 들여 컨텐트를 생산한 컨텐트 제작자/배포자에 대한 권리를 보호하고자 각 단말기에는 DRM을 설치하여 컨텐트의 부적절한 불법복제및 유포를 막으려는 노력이 진행중이다. 하지만 DRM은 국제표준이 없는 상태에서 각 업체별 자사의 독자 DRM을 사용하기 때문에 홈네트웍상에 서로 다른 업체의 단말기간 컨텐트 공유가 되지 않는다. 따라서 본 논문에서는 홈네트웍을 구성하는 이종 단말기간 안전한 컨텐트 및 라이센스 이동/복사가 가능한 전송망을 통해 컨텐트를 서로 공유할 수 있는 예를 제시한다.

2. 장. 본 론

2.1 절. 홈네트웍상에서의 멀티미디어 컨텐트 DRM 적용

홈네트웍상에서 멀티미디어 컨텐트 DRM 적용은 컨텐트의 불법복제및 유포를 막기위해 인증된 홈서버/홈가정 단말기에 한해 컨텐트 제공자로부터 서로 다른 전송경로를 통해 암호화된 컨텐트및 라이센스를 외부의 hacking 위험이 없는 안전한 전송망을 통해 전송 / 재생 / 사용제한 하는 과정이라 할 수 있다. 컨텐트의 사용제한은 컨텐트와 라이센스를 전달받은 단말기기가 라이센스 파일을 안전하게 해석하여 컨텐트 배포자의 의도/구매자의 구매조건에 맞게 컨텐트 사용에 적절한 제한이 가해지는 것이다. 따라서 홈네트웍상서의 멀티미디어 컨텐트 DRM 적용 모델은 TLS (Transport Port Layer)와 같은 안전한 전송망과 컨텐트및 라이센스를 암·복호화에 필요한 키를 안전하게 관리, 라이센스 해석및 그에 따른 사용제한, 이종기기간 멀티미디어 컨텐트 공유하는 부분으로 볼수 있다. 그림 1은 TLS망을 이용하여 홈네트웍상에서 멀티미디어컨텐트 DRM 적용 모델을 설명하고 있다.

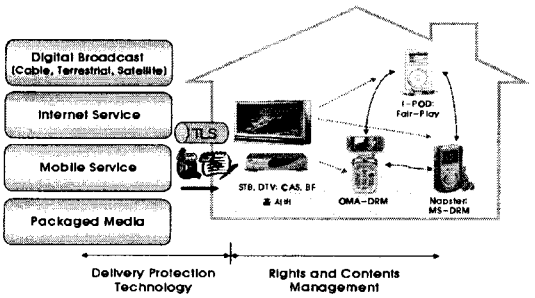
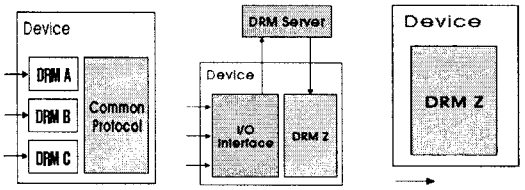


그림 1. 홈네트웍상에서의 멀티미디어 컨텐트 DRM 적용

저자 소개
* 정종진 : 成均館大學 電子工學科 碩士卒
** 김윤상: 프랑스INSAdeLyon대학 전산.생산공학과 博士卒
*** 임태범: 서강大學 전산學科 碩士卒
****이석필: 연세대학 電氣工學科 박사졸

2.2 절. DRM 상호연동 (DRM Interoperability)

DRM 상호 연동은 이종 DRM이 적용된 단말기간 컨텐트를 서로 공유가능하게 한다. 위 그림1에서 보듯 현재는 Apple사에서 적용한 Fiar-Play DRM 적용한 컨텐트는 MS-DRM이 적용된 컨텐트에 복사를 한다 하더라고 컨텐트 암호화 방법, 라이센스 파일 구성및 암호화 방법등이 다르기 때문에 재생이 불가능하다. 다시말해 지금 시장은 표준이 없는 상태에서 각 업체별 자사의 DRM을 적용하기 때문에 이종 DRM이 적용된 기기간의 컨텐트 공유는 불가능한 상태이다. 따라서 이종 DRM 단말기간 컨텐트를 공유하기 위해서는 그림2과 같은 3가지 시나리오가 있다.



a) 다수 DRM 적용 Layer　b)외부 서버를 이용　c)하나의 국제 표준 DRM 적용

그림 2. 가능한 DRM 상호연동 방법

그림 2-a)는 하나의 단말기가 모든 DRM을 지원해야 되기 때문에 시스템이 너무 커져 버리고, 로얄티 문제로 인해 단말기 제조단가가 커지기 때문에 제조업체와 구매자에게 큰 부담을 주어 시장성이 떨어진다. 그림 2-b)는 DRM 상호연동을 위해 네트웍상에 존재하는 외부서버를 이용해야 되기 때문에 항상 on-line 상태이어야 하며, 네트웍상태에 따라 성능차이가 많이 난다. 그림 2-c)는 하나의 국제표준 DRM을 컨텐트 제작자/제공자/단말기업체등이 사용하는 방법인데 iPOD와 같은 시장에 이미 널리 퍼져있는 기존의 단말기에 대한 처리문제와 회사별 DRM 정책및 시장 선점도등을 봤을때 업체에서 이를 받아들인다는 것은 불가능한 상태이다. 따라서 현재 시장에 존재하는 DRM과 추가적으로 앞으로 새롭게 생겨날 DRM을 쉽게 수용 가능하면서, DRM 상호연동을 위한 중간자 역할을 하는 모듈이 필요하다.

2.3 절.제안한 DRM 상호연동 (DRM Interoperability) 모델

홈네트웍을 구성하는 이종 DRM 단말간 상호연동을 통한 컨텐트 공유를 위해서는 현재 시장에 판매된 DRM 기기들을 포함하여, 앞으로 새롭게 생산될 DRM 적용 단말기간에 컨텐트 공유가 가능해야 된다는 문제를 해결해야 한다. 이를 위해서는 A-DRM을 해석해서 B-DRM으로 변환할 수가 있어야 하며 임의의 Z-DRM으로도 변환을 할 수 있는 모듈이 필요한데, 이는 각 회사의 컨텐트 암호화 방법및 라이센스 파일의 구성/암호화 방법이 공개된다는 점에서 각 업체들이 수용하지 않을 것이다. 또한 A-DRM을 제공하는 업체는 DRM 적용 시나리오가 다양하고 체계적인데 반해 변환될 B-DRM은 A-DRM의 라이센스 정책을 모두 반영시키지 못해 A-DRM의 컨텐트 사용제한이 B-DRM으로 변환된 경우 적절하게 제한이 안되는 경우도 있을수 있다. 따라서 그림 3은 위 상황들을 절충하여 이종 기기간 DRM 상호연동이 가능한 모델을 설명하고 있다.

그림 3에서 IntraBox와 AL(Adatation Layer)은 source 와 target 두 DRM의 중간자 역할로서 DRM A를 DRM B로 변환하기 위한 구성원들이다.

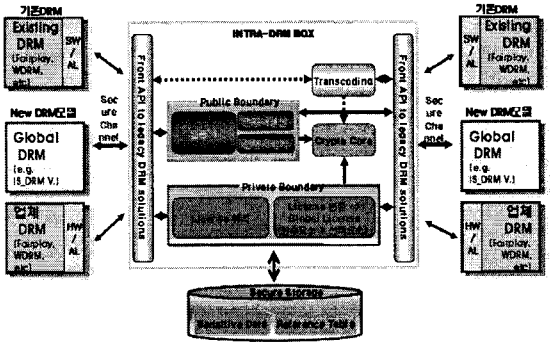


그림3. 제안된 DRM 상호연동 모델

S/W AL은 이미 시장에 퍼져있는 DRM 적용 기기들을 위한 것으로서 해당 업체 DRM을 global DRM으로 변환하기 위한 것으로서 업체들이 SW 모듈을 Firmware Upgrade등의 방법으로 기존 기기에 설치해서 사용할 수 있고, Global DRM을 적용하지 않은체 자사의 DRM을 계속 적용하는 정책으로 앞으로 생산되는 모델에 대해서는 SLM(Secure License Management)의 소형 chip을 탑재해서 위의 역할을 하면 된다. 또한 DRM에 대한 강점이 없는 업체로서는 표준으로 정한 global DRM을 적용하여 제품을 내놓으면 AL과 IntraBox를 통해 기존 DRM적용 기기, 앞으로 생산될 기기들간의 이종 DRM 상호 연동이 가능해 진다. 다만 Global DRM은 256 bit의 AES 알고리즘으로 컨텐트 암•복호화와 필수구성요소와 선택구성요소를 정의한 License파일을 정의 하여 구성하여 사용할 수 있다. 기존 DRM의 암호화키는 AL에서 IntraBox로 안전하게 전송하여 AL및 Intrabox에서 AES로 변환후 target으로 전송하면 target의 AL은 AES로 암호화된 content를 target 자사의 AES 복호화하여 재생가능하다.

라이센스 필수구성요소에서는 컨텐트 제한의 기본적인 공통요소를 구성하여 사용할 수 있고, 자사의 독특하거나 강점이 있어 시장점유가 가능, 공개가 불가능한 부분들은 선택적 구성요소에 정의하여 블랙박스화 시켜, target이 자사 DRM과 제휴된 경우에만 모든 라이센스 해석이 가능하고, 만일 그렇지 않은 경우 다른 DRM 단말기로 이동시 필수구성요소만 해석되어 기본적인 사용제한이 적용되면 된다.

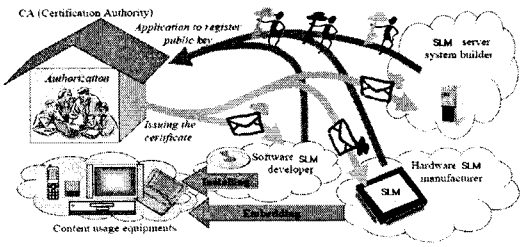


그림 4. SLM 인증 및 AL 탑재

그림 4는 HW AL에 사용되는 SLM 모듈 chip을 설계, 인증 서버로부터 인증절차를 거쳐 등록된후 각 단말기에 탑재되어 AL 기능을 담당한다.이 SLM인 intraBox와 컨텐트 및 라이센스전달시 안전한 전송프로토콜인 TLS를 이용하여 키 관리 및 session을 유지하는 역할도 담당하게 된다.

그림 5는 업체별 컨텐트 암호화 방법과 license 형식이 각 SLM AL을 거쳐 intrabox로 정달되는 과정을 설명하고 있다.

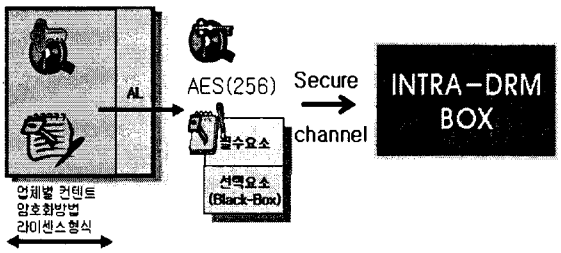


그림 5. SLM AL을 통한 컨텐트및라이센스변환

2.4 절.제안된 Global 라이센스 format

Global DRM을 적용하여 라이센스 파일을 본래 global 형식으로 작성이 되는 AL을 통해 Global 라이센스 형식으로 변행이 되는 결과물은 필수구성요소와 선택구성요소로 구분이된다. 필수구성요소에는 모든 단말기기가 컨텐트 제한을 수행할 수 있는 기본적인 내용으로 구성되고 선택요소에는 각 업체별로 제휴된 기기에서만 동작가능한 부분으로 블랙박스 형태로 구성된다. 예를 들어 Apple사의 FairPlay를 적용한 iPOD와 MS-DRM을 적용한 단말기간 서로 컨텐트 공유를 할 수 있게끔 Apple사와 MS사간 제휴가 이루어졌다만 이 두 기기간에 선택적 요소인 두 블랙박스 내용이 모두 실현 가능하지만 제휴가 이루어지지 않았다면 필수구성요소만 실현이 가능해 진다.

그림 6은 Applce사의 iPOD에 적용된 Fairplay DRM의 라이센스 파일이 AL을 거쳐 Global 라이센스파일로 변형된 하나의 예를 보여준다.

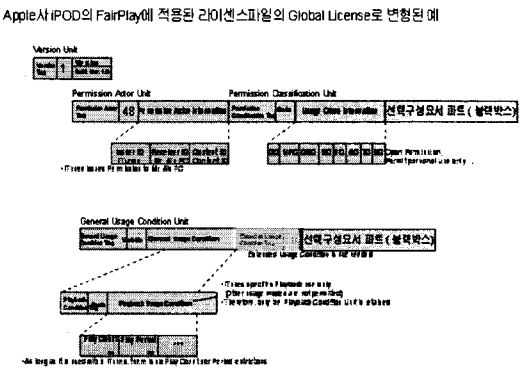


그림6. Apple사 iPOD의 FairPlay에 적용된 라이센스파일의 Global License로 변형된 예

3. 장 결 론

과거에는 인터넷으로 연결된 PC 에서만 디지털 콘텐츠의 이용이 가능하였지만 이제는 디지털 방송 및 디지털 홈 네트워킹을 통해 가전기기 또는 모바일 기기에서도 디지털 콘텐츠 이용이 확산되고 있으며, 이러한 콘텐츠들을 보호하기 위하여 다양한 디지털 콘텐츠보호 기술이 개발되고 있다. 따라서 현재까지 인터넷 기반의 PC 플랫폼을 중심으로 발전되어 왔던 DRM 기술도 디지털 방송환경 및 홈네트웍 환경의 다양한 요구사항을 만족하기 위하여 신규기술에 대한 새로운 접근을 계속 모색하고 있으며, 기존의 다양한 DRM과의 연동을 통한 멀티미디어 컨텐트의 공유가 사용자의 강한 욕구로 나타나고 있고, 컨텐트 제공업체및 단말기기 제조업자들 또한 이런 요구를 외면하기 힘들 것이다. 하지만 현재 컨텐트공유를 위한 DRM 상호 연동은 현 시점에서 모든 단말기기및 서버가 하나의 동일한 국제표준의 DRM을 적용하기란 불가능하며, 기존의 시장을 많이 점유한 업체들의 DRM을 끌어안으면서 DRM 상호연동을 추진해야 할 것이다.

DRM 상호연동 솔루션은 전적으로 권리 소유자를 배제하고, 사용자만을 위한 기술이라고 말할 수 없다. 불법적 콘텐츠 복제는 업계 수익 저하에 따른 소비자가 콘텐츠 획득을 위해 지불해야 될 비용을 증가시키는 결과를 가져다주며, 궁극적으로 보았을 때 DRM 상호연동은 저작권 소유자, 업계, 소비자 모두를 위한 솔루션이라고 할 수 있다.

본 논문에서 제시한 indrabox를 통한 DRM 상호 연동은 하나의 예를 제시할 뿐 근본적인 해결책이 되지는 않는다.따라서 시장을 장악한 주요업체들이 수긍하고 그 업체들의 DRM의 강점들을 살린체 소비자 요구를 만족하는 편리한 DRM 상호연동에 방법이 계속 연구되어야 할 것이다.

참 고 문 헌

[1] Multimedia home server systems - Conceptual model for digital rights management -DTS, June-2006

[2] Permission Code -IEC PT62227 NP, September, 2005

[3] CableLabs, CableCARD Interface Specification, OC-SP-CC-IF-C01-050331, March, 2005

[4] CableLabs, CableCARD Copy Protection system Interface Specificationtion, OC-SP-CCCP-IF-C01-050331, March, 2005

[5] FCC, Report and Order and Further Notice of Proposed Rulemaking, FCC 03-273, December, 2003

[6] FCC, FCC Order, FCC 04-193, August, 2004